SmartData Fabric® (SDF)
Data Security Layer (DSL) for AWS

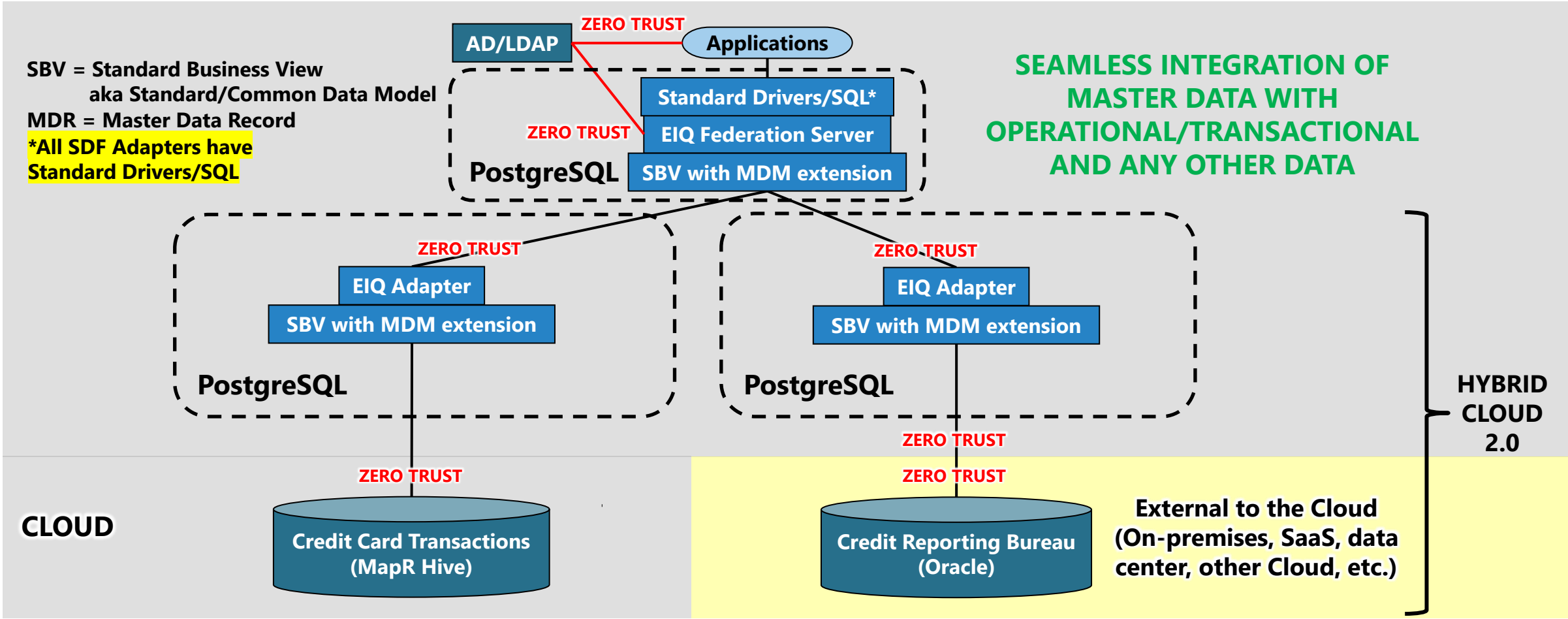
February 2024

SmartData Fabric® (SDF) enables a holistic security-first approach to data security and privacy

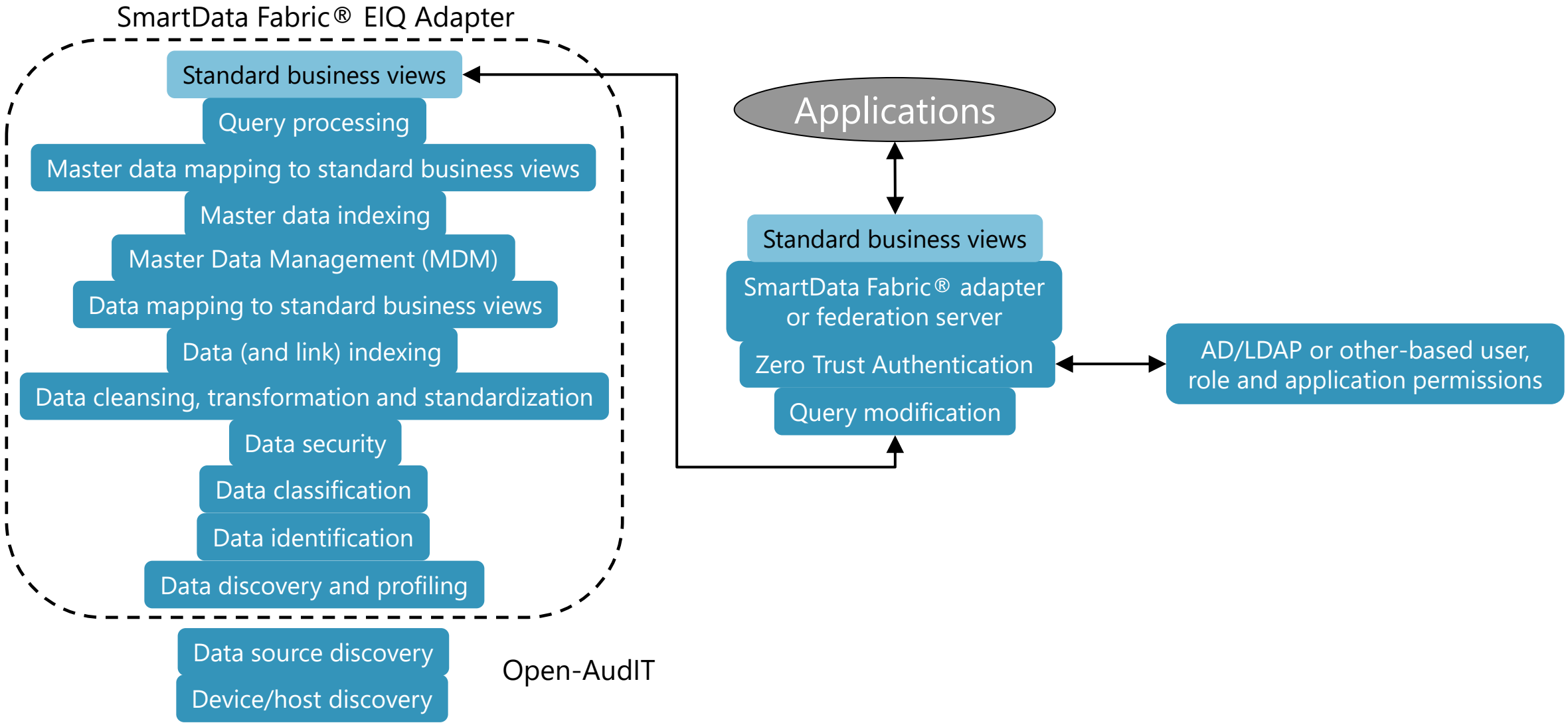
- **SDF enables and enforces Forrester® Zero Trust Data Security Framework**
  - Discovery, INDEXING, identification, classification and security
- **SDF leaves data in sources and does not copy raw data to a centralized location, e.g., data lake**
  - Greatly reduces significant risks due to unidentified, unclassified and unsecured copies of data
  - Federated architecture avoids a large-scale single point of failure
  - Edge pre-processing of data enables Data Mesh concepts with deeper local knowledge, and security and privacy closer to sources
- **SDF discovers, profiles, identifies, classifies, secures, cleans, transforms, standardizes, indexes and maps data to standard business views and objects BEFORE any queries made and results provided**
  - Dynamic masking, tokenization and/or encryption of results data, depending on user and/or role permissions, including while building AI models, embeddings and prompts
- **SDF enforces enterprise data governance policies and rules throughout, as data is discovered, pre-processed and queried**, and matches data governance with enterprise governance of user, role and application permissions
  - Bridges the gap between data, and users, roles and applications
- **SDF uses a highly advanced third-party data privacy and anonymization framework**, in addition to PostgreSQL built-in data security and privacy
- **SDF leverages AI/NLP for unstructured data** to identify and classify entities, and significant phrases in unstructured data
- **SDF supports "live or direct query" mode** to run reporting, BI, analytics, AI and other apps in a federated data architecture vs. the far more common "data extract" mode that copies some or all data without pre-processing to centralized storage for subsequent processing and queries, and increased data risks

Note: Additional data security and privacy features on slides 10 and 11 at the end of this presentation

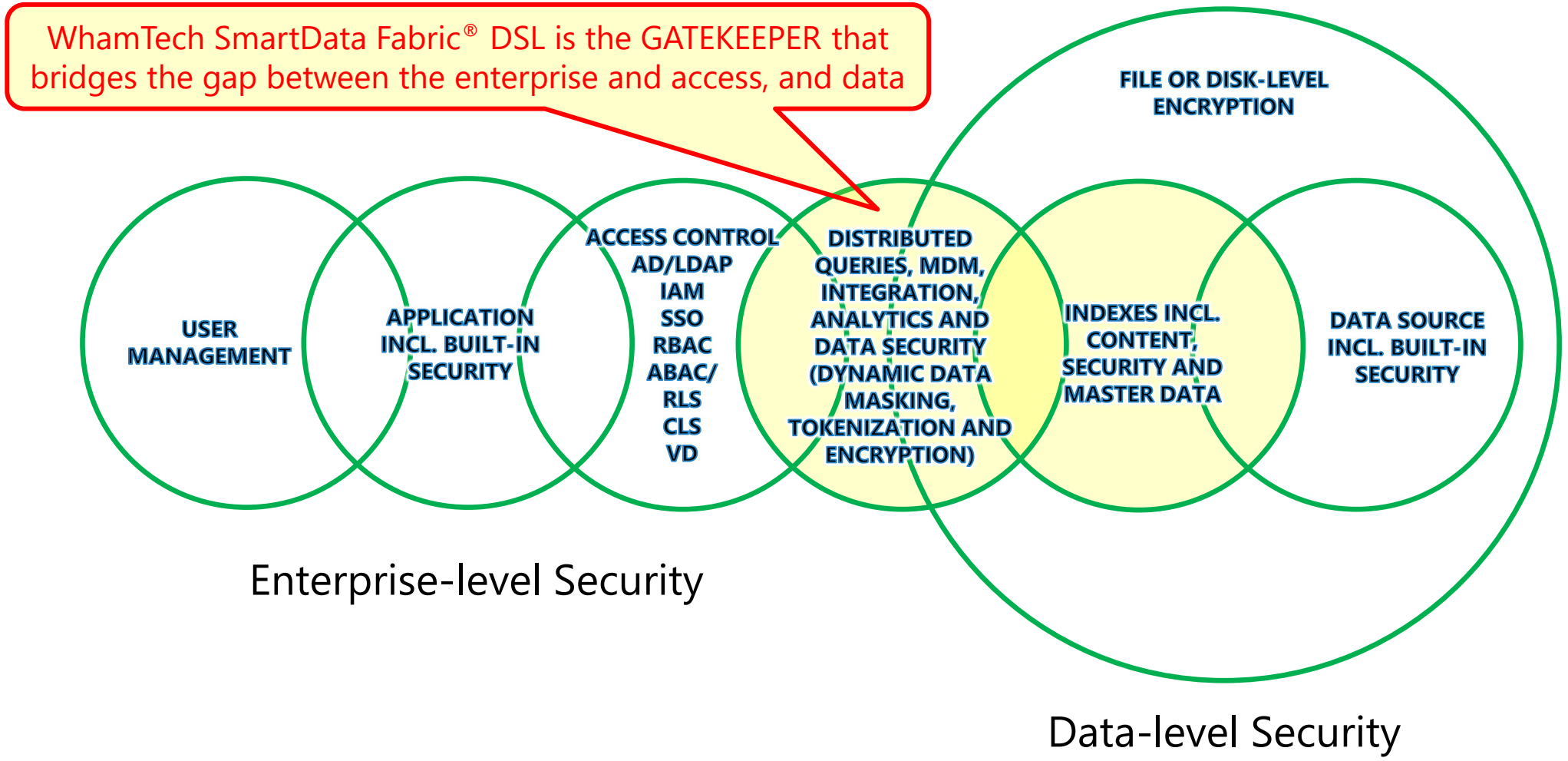
Example simple real-life cloud-based configuration



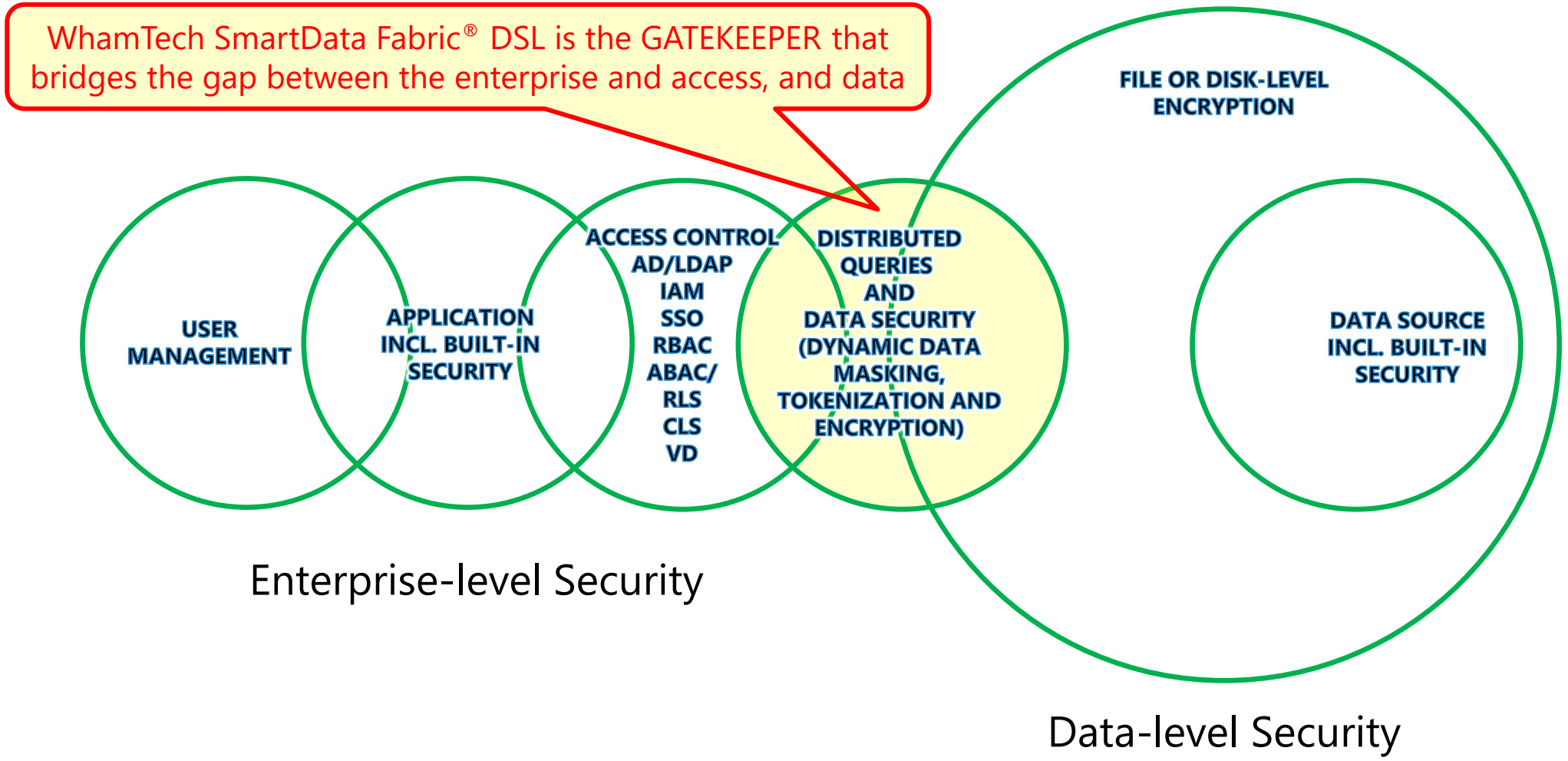
SDF enforces enterprise data governance policies and rules throughout



SmartData Fabric® Data Security Layer for indexed adapters



SmartData Fabric® Data Security Layer for conventional (unindexed) adapters



Zero Trust throughout SDF DSL, including in and outside of AWS

1. Data security through discovery, indexing, identification, classification and security (and privacy) in conjunction with policies, and highly configurable and advanced rules-based framework for data in transmission and at rest
2. Authentication and access control
3. Internal SDF identity and access management (IAM) via creating, storing, and managing user accounts that access SDF EIQ Adapters and EIQ Federation servers
4. Identify and authorize devices, apps and tools that access SDF – tie-in with endpoint management system (EMS)
5. Share Zero Trust principles with customers, including the need to secure data sources
6. Network security via configuration of adapter and federation server resources in and outside of AWS
7. Monitor, analyze all access, and provide malware protection through Amazon Guard for the adapters and federation servers in and outside of AWS

Highly advanced third-party data security, privacy and anonymization framework for PostgreSQL

Framework with extensive capabilities that address critical data security and privacy requirements:

- Rule-based framework
- Highly flexible and easy to extend
- Multitude of privacy and anonymization functions
- Default implementation for various masking and anonymization functions. Example: Obfuscation functions for first name, last name, date of birth, social security number, street address, state, zip code, salary, strings, numbers, dates, money, etc.
- Separation of masking from obfuscation
- Ability to override default implementation using rules
- Comprehensive rule types with ability to set fixed values, NULL, or use custom functions
- Ability to scope rules at user level, role level, role group level, or for all users (PUBLIC)
- Support for rule inheritance via role inheritance. NOTE: Only one rule that gives most access (or least privacy/anonymization) is applied, when in conflict
- Support for applying privacy and anonymization to new views using appropriate functions
- Auto enable existing tables and views for privacy and anonymization
- Support applying privacy and anonymization during replication
- Default functions to support auto enabling of existing tables and views for 20+ data types
- Support for custom functions with arbitrary number of input parameters and data types
- Fully configurable enabling total customization
- Integrates with custom implementation and/or a third-party anonymizer

OUTCOME:

SmartData Fabric® can apply Zero Trust data governance, data security and more, and enterprise-level access control, on ANY source system, regardless of the source system's support for any of these measures

Additional security features (1 of 2)

- **SDF enforces other Zero Trust functions** such as authentication at each level, and adheres to NIST and CIS security principles, standards and guidelines
- **SDF provides layered security**, i.e., different levels of security (authentication, access control, preventive measures, monitoring, encryption, masking, transformation and/or tokenization) are applied depending on whether data is classified as “radioactive”, “toxic”, or “unclassified”, per Forrester Zero Trust.
- **SDF will be HIPAA and HITECH-compliant**, and supports CCPA/CCPR and other GDPR-type regulations
- **SDF maps source data to standard data**, and that supports automatic data governance
- **SDF Master Data Management (MDM) ensures correct and complete datasets** are read in integrated result-sets
- **SDF can either pass through user credentials and permissions, or proxy in as different roles**, i.e., trusted infomediary

Additional security features (2 of 2)

- **SDF supports secure data at rest** – encryption of data, indexes, files, folders, directories and/or disk volumes – physical, virtual and/or logical
- **SDF supports secure data in transit** – Transport Layer Security (TLS)
- **SDF also has security indexes**, e.g., multilevel, including hierarchical access depending on user and other classifications
- **SDF can encrypt entire result-sets**
- **SDF supports GDPR and similar personal data-related regulation**s that require a bridge between logical views and physical storage of personal data, how personal data is used, and allow customers to "erase" specific personal data
- **SDF can support and enforce User Behavior Analytics (UBA)** by making available audit logs (user, query and results), in conjunction with access control, metadata, data governance and data security – virtual graph database, link analysis and visualization can also help

The End